Emory Mobile App Review and Submission Process for Internal Emory Distribution

Status of this Document

This is the current description of the Emory Mobile Application Review Process for apps bound for internal distribution to Emory people only. These may be apps for internal use at Emory or apps that will eventually be released publicly, but are in a prototype, beta, R&D, or QA phase of existence. If you are ready to submit your application for general availability release on a public app marketplace, please see the page entitled Emory Mobile App Review and Distribution Process for Public App Marketplaces. This document describes the process in use and not an ideal process. Comments and suggestions are welcomed as comments on this page, or you may send feedback to Steve Wheat at <swheat@emory.edu>.

Step 1: Request Internal Distribution of the Application

In order to review an app for internal distribution, a mobile app must first be distributed to the internal Emory reviewers using the Emory Mobile App Catalog. Complete the Internal Mobile App Distribution Request Form to start the process. A mobile app can usually be distributed internally to a restricted group in two or three days from the time of the request. Distribution to a large internal audience usually take two to three weeks to complete the internal review process, and distribution on public marketplaces may take several weeks to several months depending on the complexity of the app and the compliance and commercial implications of the app.

Step 2: Internal Posting Review

Emory Library and Information Technology (LITS) performs a high-level technical review of the application to determine if there is a need for any detailed security and compliance reviews of the application. For example, if the application collects and stores ePHI, credit card information, or other compliance related data, Emory LITS will inform the owners of the application of relevant policies and any practices required by those policies. See the template for this cursory review. LITS will create a copy of the review template specifically for the requested application review and ensure the application owners have access to the template to complete the information. LITS staff will help complete this template as needed.

Step 3: Compliance and Regulatory Review

Emory University and Emory Healthcare compliance officers review the mobile application to determine whether or not Emory's HIPAA compliance or other appropriate compliance policies apply. Emory's compliance officers provide the following general guidance in determining whether or not HIPAA applies to a mobile application:

1. If the mobile application collects, stores, or transmits personal health information for the personal use of the consumer and not for Emory people in their role as researcher, clinician, or support role, then HIPAA does not apply to the application.
2. If such an application provides Emory researchers or clinicians access to the personal health information for the purposes of research or patient care, then HIPAA does apply to the application.
3. All such applications that collect, store, or transmit personal health information must implement appropriate information security measures to protect personal health information, regardless of whether or not Emory's HIPAA compliance policies apply.
4. Emory Information Security has compiled a list of mobile app defaults and mobile app specific security review questions that must be considered when designing, developing, and distributing mobile apps.

Step 4: Technical & Information Security Reviews

Using the answers to the mobile app security questions, Emory LITS performs a high-level technical review of the application to determine if there is a need for any detailed security and compliance reviews of the application. For example, if the application collects and stores ePHI, credit card information, or other compliance related data, Emory LITS will inform the owners of the application of relevant policies and any practices required by those policies. Additional materials may be required, depending on the type of review specified. The organizer of the technical review team will contact application developers and help them prepare any additional materials.

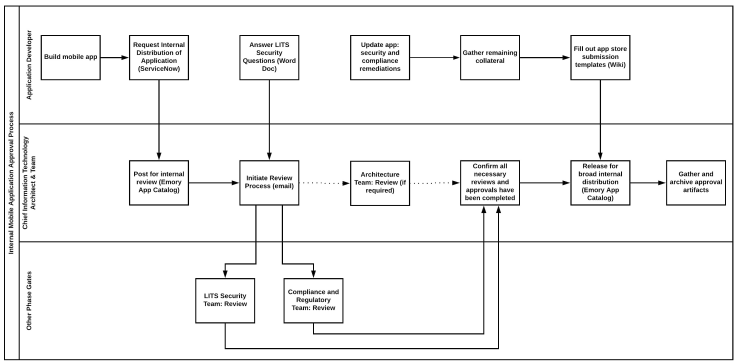
If an in-depth security review is required, a meeting is scheduled with representatives of Emory Information Security to walk through a mobile app security checklist based on the security, compliance, and regulatory requirements that are relevant to the particular application.

Subsequent App Update Submissions

For subsequent application updates, application owners should update the technical review template and if there are substantial changes, request another review. For example, if the nature of the data being collected or stored by the application has changed and now ePHI is being collected when it was not before, then a new review should be scheduled. Application owners should also update the internal submission forms relevant to their applications for each subsequent submission.

Internal App Review and Distribution Process Flow

Please on click the image below to enlarge.


Internal Mobile Application Approval Process
Application Developer
Chief Information Technology Architect & Team
Other Phase Gates
Build mobile app
Request Internal Distribution of Application (ServiceNow)
Answer LITS Security Questions (Word Doc)
Update app: security and compliance remediations
Gather remaining collateral
Fill out app store submission templates (Wiki)
Post for internal review (Emory App Catalog)
Initiate Review Process (email)
Architecture Team: Review (if required)
Confirm all necessary reviews and approvals have been completed
Release for broad internal distribution (Emory App Catalog)
Gather and archive approval artifacts
LITS Security Team: Review
Compliance and Regulatory Team: Review